Information Security & Privacy

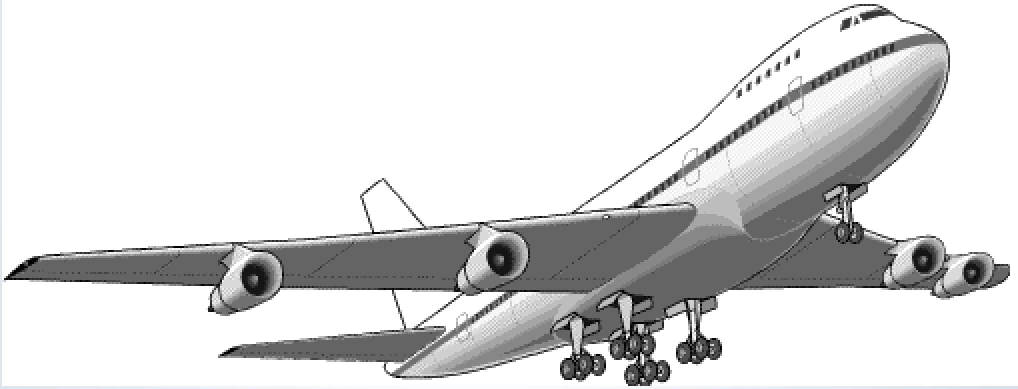
ISPAB Meeting
September 5th, 2008

Deven Bhatt, CISA, CISM, CISSP
CSO
Airlines Reporting Corporation

A·R·C

Airlines Reporting Corporation

ARC - is an airline-owned company serving the travel industry with financial services, data products and services, ticket distribution, and settlement in the United States, Puerto Rico and the U.S. Virgin Islands.



ARC Proprietary.

Overview of ARC

- $77+ billion settlement last year
- 20,000+ Accredited travel agencies
- 150+ Corporate Travel Department locations
- 170+ Participating global carriers
- 18 System Providers

Governance

- CSO reporting to the President & CEO
- Converged - Information & Physical security, Privacy
- Funding - budget
- Developed new security program and team
- Enterprise Architecture Review Board

Risk

- Identify Risks
- Map with Company Strategic Plan
- Initial quantitative analysis - score
- Mitigation (Approval for funding)
- Review resulting Risk scores

Compliance

- Most companies have to comply with multiple regulations
- Payment Card Industry Data Security Standard*
- EU Safe Harbor
- First to be compliant in travel industry
- First in the world to encrypt Teradata
- Internal compliance effort is “Continuous”
- Save money & effort - Combined PCI and Internal Audits
- Proactive and holistic approach (No checklist)

Note: PCI DSS copy rights are owned by PCI Security Standard Council

People First - Awareness

Sec_rity is incomplete without "U"

- Mandatory attendance to CSO presentation
- Web based, online class
- Personal safety and Identity Theft
- Awareness Event with fun themes (Jeopardy)
- Brochure with security team cell phone nos.
- Teaser movie - CEO (Mission Impossible), CFO participation
- Fun - CSO - Inspector Clouseau
- CSO briefings at monthly staff meetings

ARC Data Security Standard

- All PCI requirements – included as baseline
- Raised The Bar (added more controls)
- Reviewed ISO 2700X, and other frameworks

ARC Proprietary.

Protect Confidential data

- Discover where the data is, who has access
- Classification
- Retention
- Data going out (Highest risk)
- Data at rest
- PII (Personally Identifiable Information)

Technology Hot Topics

- Encryption - laptops\desktops, email, database, mainframe, backup tapes, and CD
- Log and security event management
- Application Layer Firewall (PCI 6/30/2008)
- Code review
- Agile and Secure coding – OWASP, Payment Application Data Security Standard*
- Data Loss Prevention (Storage, Transit, End Point)
- Virtualization

Note: PA DSS copy rights are owned by PCI Security Standards Council

Identity and Access Management

Access Control

- User Provisioning - ARC Identity Manager
- Data Steward approval – Justification – Periodic Reviews

Stronger authentication

- Enterprise Directory (LDAP) to support Portal and application integration

ARC Proprietary.

Physical Security

- Centralized access control
- Cameras\Digital Video Recorders
- Strict identification and access
- Strong authentication (2 factor – PIN\Biometric)
- Shredding, supervised destruction of media

NOTE: “Social Engineering” attack education

Monitoring

Track & monitor access

- Security Event Monitoring solutions
- Real time blocking and sending alerts
- Database monitoring
- Capture complete user session

Regular testing

- Internal (Dedicated resources)
- External scanning (Approved Scanning Vendor – SaaS)
- IDS/IPS (at multiple levels – Defense In Depth)
- Lead CSIRT meetings, review breaches and incidents

Policies

- Develop, Educate, Enforce
- Simplify, Consolidate, Update
- Acknowledgement
- Investigate violations, report to HR for action
- Monthly Review with President & CEO
- Third party compliance, contract review, audit

Positive Results

- Business enabler for critical projects (e.g. Prepaid MasterCard Travel card offered by ARC)
- “Best In Class” – Leader, SANS Security Summit, CSO\CISO forums, Case studies – Aberdeen, PCI Security Standard Council, Hospitality Industry conference
- Competitive Differentiator in RFP
- Final on site audits are easier, BoD, Audit committee

- Winner 2007 CSO magazine Compass Award
- Winner 2008 TDWI “Data Governance”

Thank you.

Deven Bhatt

dbhatt@arccorp.com

ARC Proprietary.